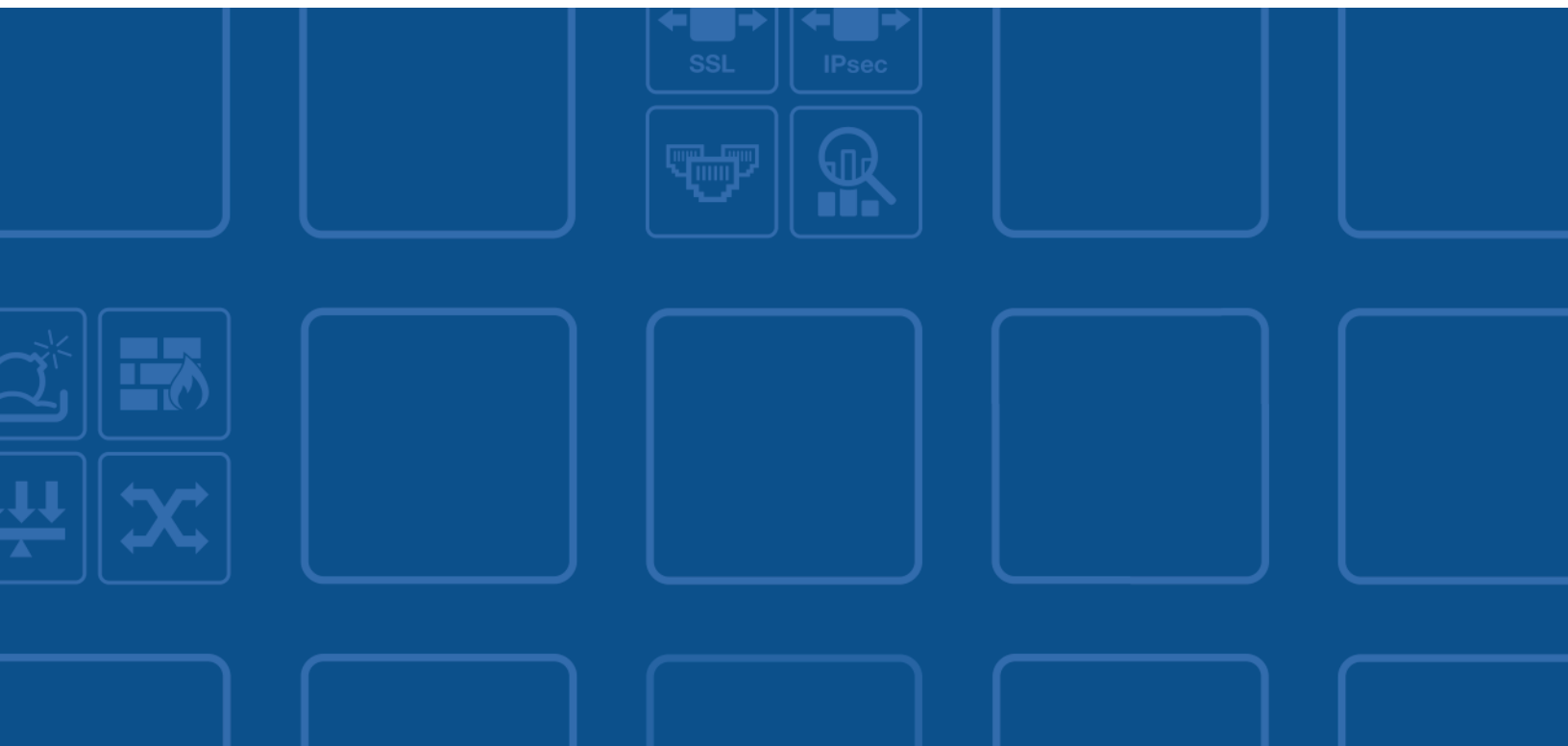
FORTINET
High Performance Network Security

FortiClient (Windows App) - User Guide

VERSION 1.0



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

February 23, 2018

FortiClient 1.0 (Windows App) User Guide

04-100-370210-20180223

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
FortiClient (Windows App) features 5
SSL DNS server and DNS suffix 5
Supported platforms 5
Initial Configuration **7**
Download the installer 7
Running FortiClient (Windows App) 8
To add a VPN connection: 8
To connect to a VPN connection: 11
To disconnect from a VPN connection: 13
To edit or remove a VPN connection: 13

Change Log

Date	Change Description
2016-05-02	Initial release of 1.0.0.
2016-09-06	Updated "Supported server address formats" on page 10.
2016-09-07	Added an *Ignore server certificate* note to "To connect to a VPN connection:" on page 11.
2016-09-12	Initial release of 1.0.1.
2017-03-08	Added "SSL DNS server and DNS suffix" on page 5.
2018-02-23	Release of single merged document for 1.0 releases.

Introduction

FortiClient is an all-in-one comprehensive endpoint security solution that extends the power of Fortinet's Advanced Threat Protection (ATP) to end user devices. As the endpoint is the ultimate destination for malware that is seeking credentials, network access, and sensitive information, ensuring that your endpoint security combines strong prevention with detection and mitigation is critical.

This guide describes how to install and set up FortiClient (Windows App) for the first time.

FortiClient (Windows App) features

Feature	Description
SSL VPN (Tunnel Mode)	SSL VPN in Tunnel Mode supports the following: • Full tunnel & split tunnel (IP and subnet based) • SSL realm, custom DNS server, DNS suffix • Username & password authentication • PKI user with a personal certificate, FortiToken & Client Certificate

SSL DNS server and DNS suffix

Example to configure SSL DNS server and DNS suffix by using FortiOS:

```
config vpn ssl settings
   set dns-suffix
"domain1.com;domain2.com;domain3.com;domain4.com;domain5.com;domain6.com;domain7.com;domai
    n8.com"
   set dns-server1 10.10.10.10
   set dns-server2 10.10.10.11


config vpn ssl web portal
   edit "full-access"
      set dns-server1 10.10.10.10
      set dns-server2 10.10.10.11
      set split-tunneling enable
```

Supported platforms

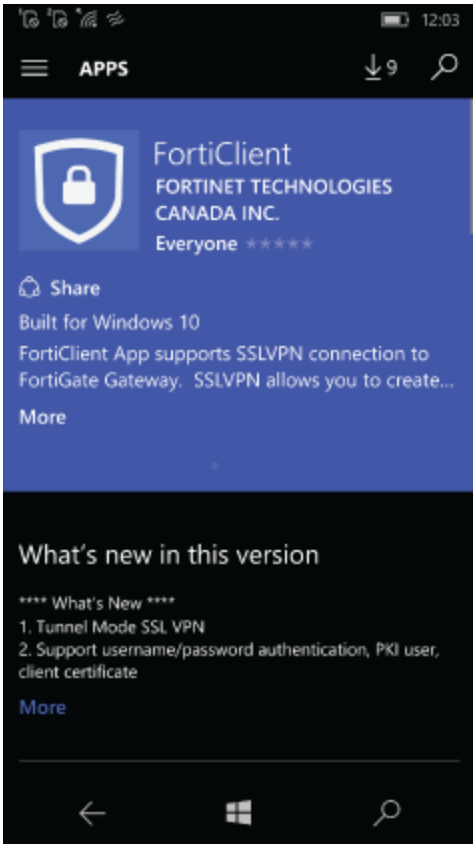
FortiClient (Windows App) supports the following operating systems:

- Windows 10
- Windows 10 Mobile

FortiClient (Windows App) requires FortiOS 5.2.4 or higher.

Initial Configuration

Download the installer



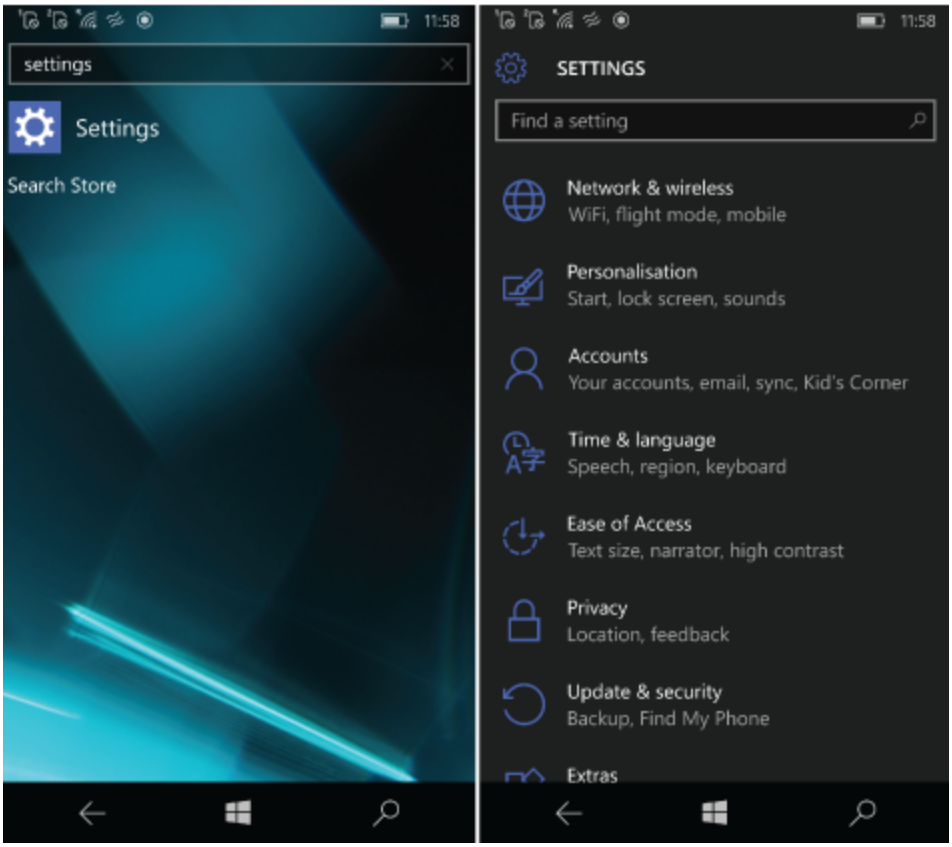
FortiClient (Windows App) is available for download from the:

- Microsoft Store: https://www.microsoft.com

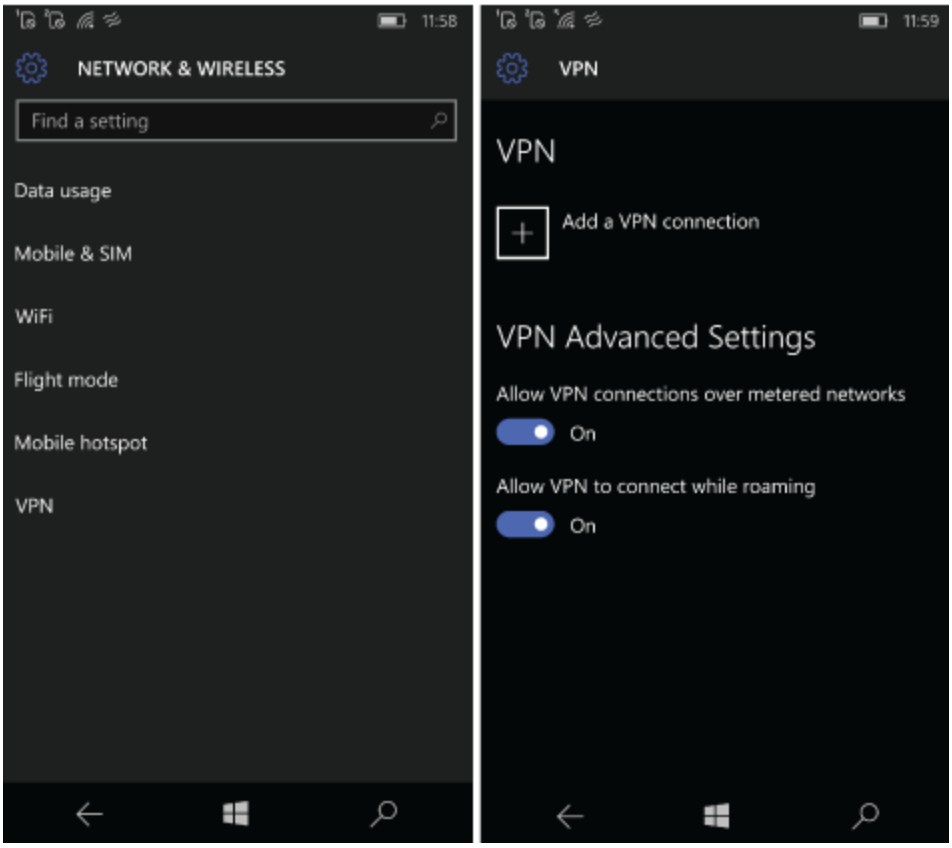
Running FortiClient (Windows App)

To add a VPN connection:

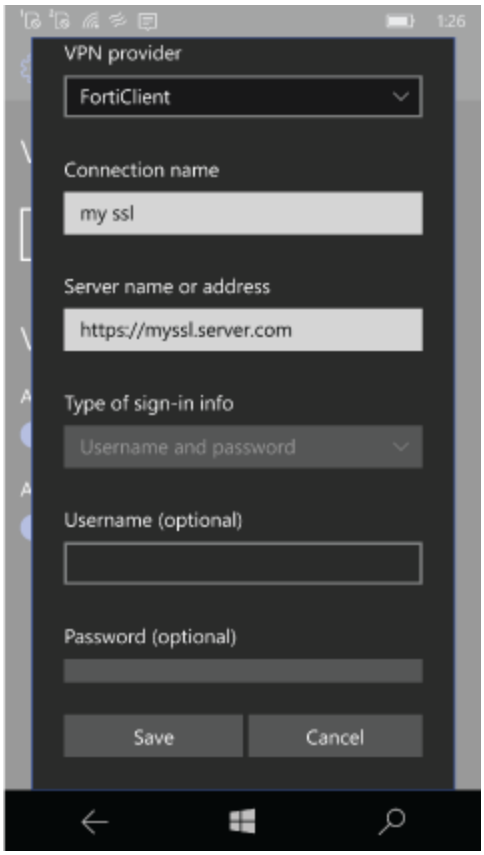
1. Go to *Settings*.



2. Tap *Network & Wireless*.
3. Tap *VPN*.



4. Tap *Add a VPN connection*.
5. Configure the following:



VPN Provider	Select FortiClient.
Connection Name	Enter a name for the connection.
Server name or address	Enter the server. A list of supported server address formats is provided below.
Type of sign-in info	Leave as is. Do not enter any information.
Username (optional)	Leave as is. Do not enter any information.
Password (optional)	Leave as is. Do not enter any information.

7. Tap *Save*.

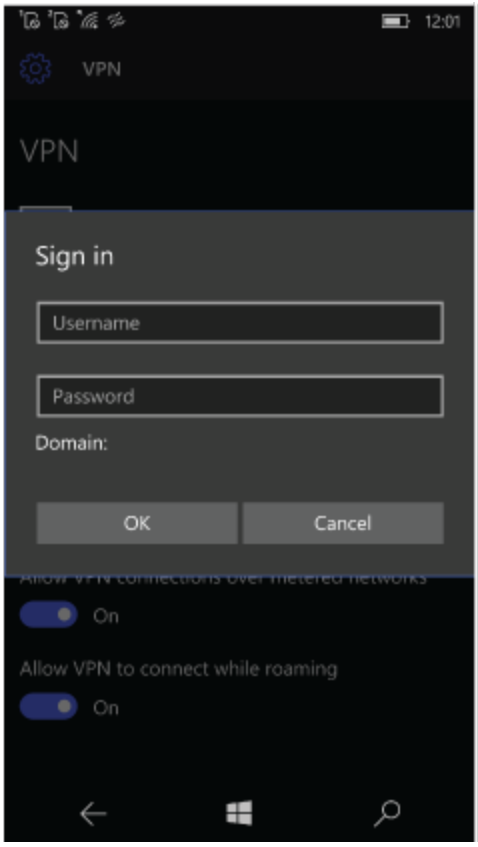
Supported server address formats

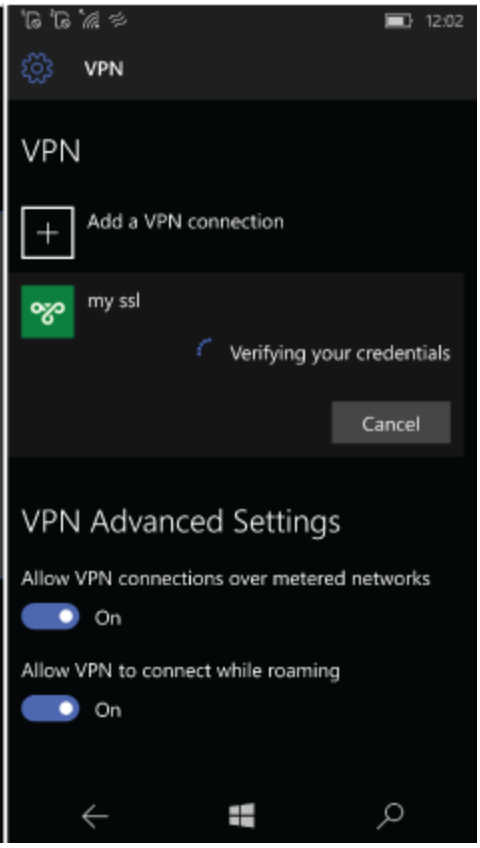
To use default port 443	• https://vpn.server.address.com/
To use a custom port (e.g. 10443)	• https://vpn.server.address.com:10443

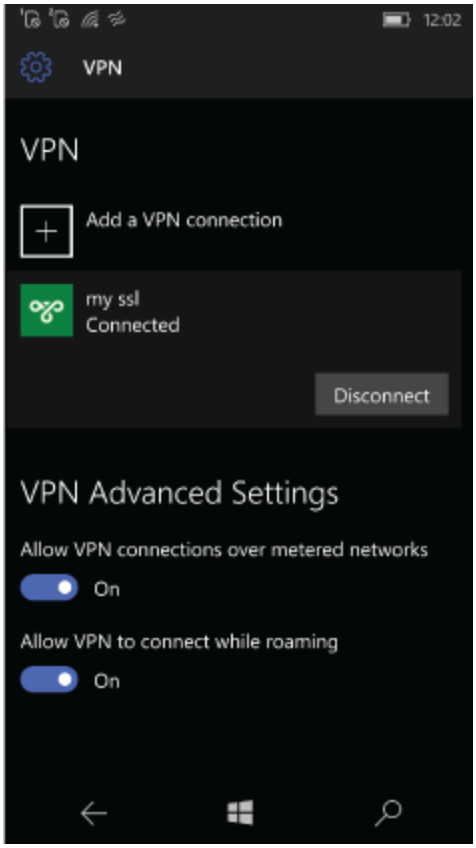
To use a realm (e.g. `realm-name`)	• https://vpn.server.address.com/realmname
A combination of customer port and realm	• https://vpn.server.address.com:10443/realmname
Ignore server certificate error	• https://vpn.server.address.com/?ignore-certificate-errors=1 • https://vpn.server.address.com/?ice=1 • https://vpn.server.address.com/?ice
Enable pop-up to select the client certificate	• https://vpn.server.address.com/?cert=
Pre-configure a client certificate	• https://vpn.server.address.com/?cert=client Where client is a substring of the certificate subject.
Use a PKI user (certificate user)	• https://vpn.server.address.com/?cert=&no-username-password=1 • https://vpn.server.address.com/?cert=&nup=1 • https://vpn.server.address.com/?cert=&nup

To connect to a VPN connection:

1. Tap a *VPN connection*.
2. Tap *Connect*.
3. Enter your *Username* and *Password*.


12:01
VPN
VPN
Sign in
Username
Password
Domain:
OK
Cancel
On
Allow VPN to connect while roaming
On


12:02
VPN
VPN
Add a VPN connection
my ssl
Verifying your credentials
Cancel
VPN Advanced Settings
Allow VPN connections over metered networks
On
Allow VPN to connect while roaming
On


12:02
VPN
VPN
Add a VPN connection
my ssl
Connected
Disconnect
VPN Advanced Settings
Allow VPN connections over metered networks
On
Allow VPN to connect while roaming
On

4. Tap *OK*.

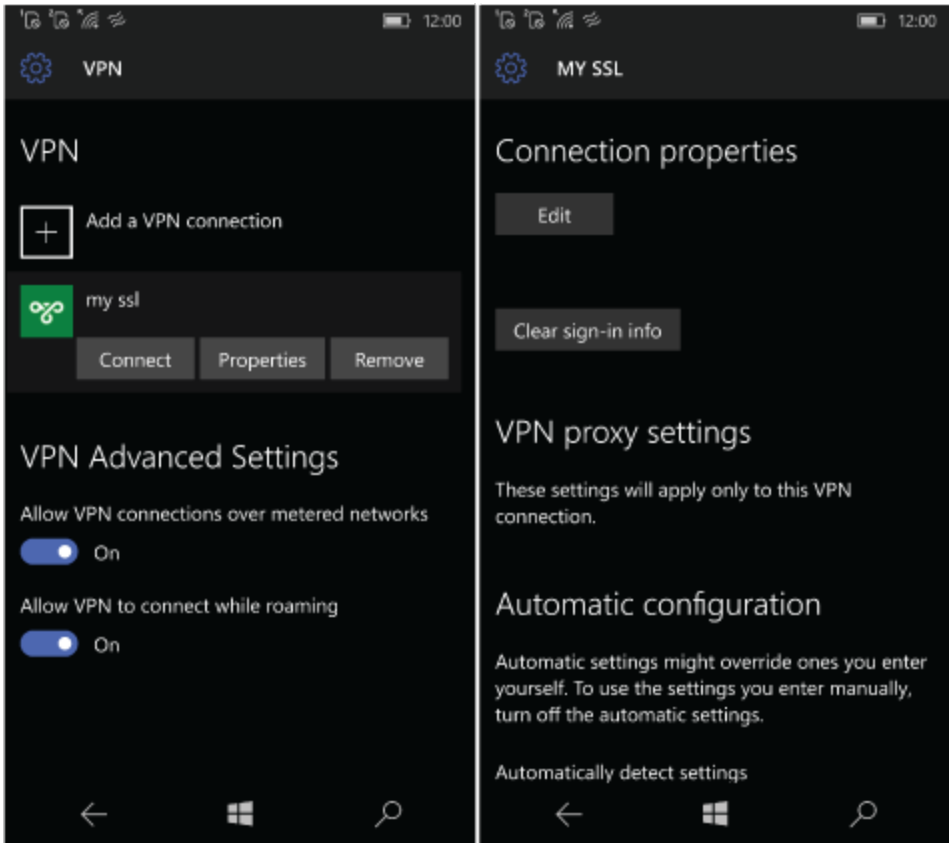
A certificate error can cause the *Sign In* screen to continuously display even when you use the correct username and password to connect to the network by using a VPN connection. You can instruct the VPN configuration to ignore the certificate error by using the *Ignore server certificate* feature. See the Supported Server Address Formats section.

To disconnect from a VPN connection:

1. Select the VPN connection.
2. Tap *Disconnect* to disable the VPN connection.

To edit or remove a VPN connection:

1. Select a VPN connection.



2. Tap *Properties/Remove*.
3. Tap *OK* to save the settings.

FORTINET®

High Performance Network Security